MAY 20, 2020

Legaltech® news

ONLINE

An ALM Publication

When Work from Home Becomes the Norm, BYOD Takes On New Complexity and Risk

Shortfalls in strong policy and information governance isn't exactly a new issue, but the current situation has exacerbated corporate risk exposure significantly. Here's a list of key areas to consider that may help focus efforts.

BY DEANA UHL AND VANESA HERCULES, FTI TECHNOLOGY

An estimated 58 percent or more of American knowledge workers are now working remotely. This number is up by more than 30 percent from pre COVID-19 averages, and dwarfs previous figures that reported roughly seven percent of the U.S.'s 140 million civilian employees worked from home. To many, this mass exodus from the conventional workplace has been a welcome shift in employer expectations and telework policies. For organizations that don't typically allow remote work, however, enabling it at a moment's notice has raised serious logistical, compliance and security challenges.

Many companies in technology, insurance, professional services and certain other industries already have a large portion of employees who work from home at least some of the time. These were relatively well prepared for the current circumstances. Others have been caught completely off guard, unprepared and without the proper equipment for tens, hundreds or thousands of employees, or infrastructure to enable them to access company systems securely from dispersed locations.

From a governance standpoint, policies that dictate the rules for working from home—including how employees interact with company data, what devices and applications are approved and what additional safety measures they need to take—are also lacking. The result is a significantly increased number in employees using personal devices for work, and the rise of new and unexpected areas of legal, security, compliance and privacy risk.

Shortfalls in strong policy and information governance isn't exactly a new issue. But the current situation has exacerbated corporate risk exposure significantly. For teams in reactive mode, working to put out fires and close the gaps in company exposure, we've compiled a list of key areas to consider that may help focus efforts. These include:

VPN use: An April CNET article reported, "Demand for VPNs increased by 44 percent over the second half of March and remains 22 percent higher than pre-pandemic levels." VPNs help employees securely access systems, but they also come with inherent challenges. For one, employees may not know how to use a VPN, or understand the proper procedures for connecting to it from their personal devices. Increased usage is also straining company VPNs and internet service providers, making it difficult or impossible in some cases for the entire remote workforce to access the network. This may force employees to use their home wi-fi or unsecured hot spots, which can lead to exposure. More, VPNs have a history of being

Illustration by Gordon Studer.

exploited by malicious actors, and some providers have been flagged for weak security. It's critical for organizations to properly vet their VPN providers and get a handle on the scope of issues surrounding VPN use to ensure the most secure connection possible for remote employees.

Information security awareness: Even employees who have been adequately trained on information security best practices may not think of security in the context of working in their homes. More than ever before, sensitive information and communications are dispersed across personal devices and residences. Employees will be taking phone calls and printing confidential documents at home; and saving privileged and private information to their personal computers and mobile devices. Awareness campaigns and best practice refreshers can go a long way in preventing private documents from being disposed of improperly or left out for others to see.

Personal networks and accounts: The merging of work and home environments will inevitably lead to more blending of company information in personal email and messaging accounts, and across smaller, less secure telecom networks. When employees use personal accounts to view and share company documents containing personally identifiable information and IP, tracking and managing that data can become very messy.

Organizations subject to data privacy laws like GDPR and the California Consumer Privacy Act may run into issues with data subject access requests and other privacy compliance matters if sensitive data resides in unknown devices and accounts. When business as usual resumes, legal, compliance and IT teams will need to remediate employee devices, to ensure private information does not remain in unauthorized or unknown locations.

Policy updates: Going forward, organizations need to revisit the BYOD policies they were developing five years ago. It's likely that we'll see a second wave of coronavirus related shutdowns later this year, and organizations need to be better prepared in round two. Ironing out what rights the company has to personal devices used for work, and processes for recalling data stored on those devices will be critical in reducing risk for future privacy, regulatory and e-discovery matters.

Process improvements: In the aftermath of this crisis, organizations can seize an opportunity to examine their weaknesses and bolster processes around them. This may include creating a centralized location to store documents, file sharing systems and policies, tracking mechanisms to monitor where data is being shared or downloaded, usage parameters for collaboration and chat applications and procedures for remediating sensitive data from remote devices.

Educate and train: The best way to ensure private and sensitive information doesn't perpetuate on personal devices is to give employees clear guidance on what they need to do when they return to the workplace. Teach employees how to find and delete sensitive information from their devices, or how to transfer it back to the company. Make sure they are equipped with the knowledge and techniques they need to help reduce risk and work from home in a secure and compliant manner.

Ultimately, companies need to be more proactive about the future of work. We're likely to see a significant increase in the number of people who continue working remotely even after the pandemic is over. Organizations need to be thinking about this shift and begin taking steps to adapt to it. Collaboration across stakeholders in legal, compliance, IT and security will be essential to meet new challenges in remote work situations, and balance employee efficiency with strong data protection.

Deana Uhl *is a managing director at FTI Consulting, advising corporate clients, with a focus on designing, implementing and enabling change management for information governance, data privacy, data security and e-discovery programs.*

Vanesa Hercules *is a senior director at FTI Consulting where she helps clients operationalize information governance initiatives, streamline litigation hold and eDiscovery processes, remediate legacy data, manage global data privacy risk, and develop cross-functional workflows with sustainable business processes.*